

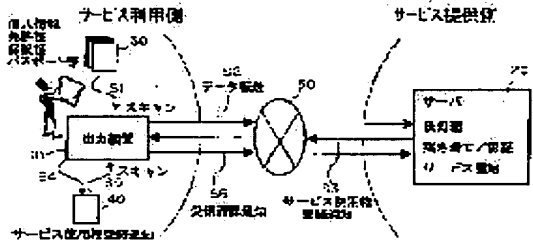
PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259716
 (43)Date of publication of application : 13.09.2002

(51)Int.Cl.	G06F 17/60 G06F 12/14
(21)Application number : 2001-053372	(71)Applicant : RICOH CO LTD
(22)Date of filing : 28.02.2001	(72)Inventor : MURATA MIKUNI KEGI SHUNZO TANIGAWA TETSUO

(54) SERVICE USER IDENTIFYING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To establish a service user identifying method for an information providing service using a network in which a service provider issues a service use right acceptance notification to allow any service user to use only a certain service (no password entry) to serve for identification of the service user.
SOLUTION: An output device 10 having a reading function and a server 20 are connected through the network 50, and the output device 10 reads the ID card 30 such as driver license, insurance certificate, passport, etc., (S1), and sends the read ID card 30 to the server 20 through the network 50. The server 20 makes checkup and verification between the individual information contained in the ID card 30 and the previously registered individual information of the service user, and if the data are identical, the service use right acceptance notification is sent to the output device 10 and the service user is identified.



LEGAL STATUS

- [Date of request for examination]
- [Date of sending the examiner's decision of rejection]
- [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
- [Date of final disposal for application]
- [Patent number]
- [Date of registration]
- [Number of appeal against examiner's decision of rejection]
- [Date of requesting appeal against examiner's decision of rejection]
- [Date of extinction of right]

(19) 日本国特許庁 (JP) (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-259716

(P2002-259716A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. ⁷	G 0 6 F 1 7 / 6 0	識別記号	F I	5-750-1 (参考)
		3 0 2	G 0 6 F 1 7 / 6 0	3 0 2 E 5 B 0 1 7
		3 2 6		3 2 6
		3 3 0		3 3 0
		5 1 2		5 1 2
	1 2 / 1 4	3 2 0	1 2 / 1 4	3 2 0 C
			審査請求 未請求	請求項の数 5 O L (全 8 頁)

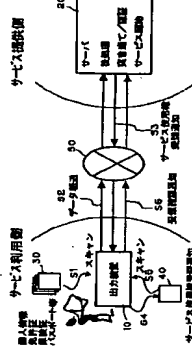
(21) 出願番号	特開2001-53372 (P2001-53372)	(71) 出願人	000008747 株式会社リコー
(22) 出願日	平成13年2月28日 (2001.2.28)	(72) 発明者	村田 巳智 東京都大田区中馬込1丁目3番6号 会社リコー内
		(72) 発明者	毛木 健三 東京都大田区中馬込1丁目3番6号 会社リコー内
		(74) 代理人	10007843 弁理士 高野 明正 (外2名)

(54) 発明の名称 サービス利用者特定方法

(57) 【要約】

【課題】 ネットワークを利用した情報提供サービスにおいて、サービス提供者がサービス利用者に当該サービスの使用可能なサービス使用権受渡通知を発行（パスワード入力なし）、サービス利用者を特定する。

【解決手段】 読み取り機能を有する出力装置10とサーバ20は、ネットワーク50を介して接続され、出力装置10は、免許証、保険証、パスポート等の身分証明書30を読み取って（S1）、読み取った身分証明書30をネットワーク50を介してサーバ20に送信する。サーバ20は、送信された身分証明書30の個人情報と予め登録しているサービス利用者の個人情報とを突き当て/照証を行って、データが合致した場合に、出力装置10にサービス使用権受渡通知40を送信し、サービス利用者を特定する。



【特許請求の範囲】

【請求項1】 MFP、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、読み取り機能を有し、サービス利用者がサービス提供者の提供するサービスを利用する際に、サービス利用者自身の免許証、保険証、パスポート等の公的な身分証明書を読み取り、読み取った身分証明書の記載内容をネットワークを介して前記サービス提供側装置に送信し、送信された身分証明書の記載内容に基づいてサービス提供者がサービス利用者を特定することを特徴とするサービス利用者特定方法。

【請求項2】 請求項1において、前記出力装置または前記サービス提供側装置は、複数の情報を自動認識する機能を有し、前記身分証明書に認識されている複数のID情報と、自動認識された複数のID情報とを照合し、前記サービス提供側装置により読み取ったサービス提供側装置に登録されているサービス利用者のID情報とを照合し、読み取ったサービス提供側装置により読み取ったサービス提供側装置に登録されているサービス利用者を特定するサービス利用者特定方法。

【請求項3】 請求項1において、前記身分証明書の記載内容に基づいてサービス提供者によりサービス利用者が特定されると、当該サービスのサービス受託を承認するためのパスワードが前記サービス提供側装置により生成され、前記出力装置は、紙出力機能を有し、該生成されたパスワードを前記サービス提供側装置からネットワークを介して受信し、受信したパスワードを紙に出力し、サービス利用者が当該サービスを利用する際に、前記出力した紙に認識されたパスワードを読み取り、読み取ったパスワードをネットワークを介して前記サービス提供側装置に送信し、送信されたパスワードに基づいてサービス提供者がサービス利用者を特定することを特徴とするサービス利用者特定方法。

【請求項4】 請求項3において、前記サービス提供側装置は、前記パスワードを、前記出力装置の読み取り機能により読み取り可能な状態で符号化することを特徴とするサービス利用者特定方法。

【請求項5】 MFP、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、携帯端末装置に関する固有情報を受信可能なFAX受信機能を有し、サービス利用者が携帯端末装置を用いて当該サービスを利用する際に、サービス利用者の携帯端末装置に関する固有情報を公衆回線を介して受信し、受信した携帯端末装置に関する固有情報をネットワークを介して前記サービス提供側装置に送信し、送信された携帯端末装置に関する固有情報に基づいてサービス利用者を特定する。

【発明の詳細な説明】

【0001】 本発明は、サービス利用者特定方法、より詳細には、ネットワークを利用した情報提供サービスにおけるサービス利用者特定方法に関し、読み取り機能を有するMFP、プリンタ等の出力装置を利用したシステムに関する。

【0002】 【従来の技術】 従来技術に関して、例えば、特開平11-338658号公報（データ管理システム）には、管理処理する処理データをユーザビリティの高いデータ処理装置に出力できるようにして、処理データを管理しているが、機器固有情報のみを管理するために、サービス利用者の特定が困難という問題点がある。

【0003】 また、特開2000-20471号公報（情報機器ネットワークシステム、その照会方法、情報機器および記憶媒体）には、各機器からユーザ情報の確認をサーバに行わせることで、ユーザ情報管理の時間的損失を減らす情報機器ネットワークシステムが記載されており、オペレータ（利用者）がパスワードを入力すると、第三者から取られ、盗用される危険の回避が困難という問題点がある。

【0004】 【発明が解決しようとする課題】 現在、IT環境の発達により、PCやMFP、プリンタが普及されたオフィスや自宅だけでなく、例えば、ビジネスコンビニエンスストアやコンビニエンスショップといった公共の場所に移動中に立ち寄るモバイルワークカーが、店内に設置されているMFP、プリンタ等の出力装置を用いてハードコピーの形態で情報やチケット等の有価証券を入手可能なサービスが行われようとしている。

【0005】 上記サービスを実施する際、サービス提供者は、情報や有価証券の対価として課金を行うことや、後の請求・回収にまつわるトラブルの発生防止やトラブル発生時の紛争解決を目的に課金内容の証明を行う必要があるため、支払い者となる利用者や契約者を特定する必要がある。

【0006】 その手段として、利用者がサービスを受け、事前にサービス提供者と利用者が共有化したパスワードを入力することが一般的である。しかし、公共の場所において、例えば、有価証券の偽造といった悪用を避けるため、周囲を盗撮することができないこともあり、そこに設置されるカラー出力機器に10キー等を入力するときに、第三者から覗かれ、盗用される危険が回避できない。

【0007】 代替手段として、例えば、磁気を用いた不可視情報により利用者情報を記録したIDカードを、サ

サービス提供者から利用者に対して事前に提供し、利用時に読み取り装置が利用者の情報を読み取り、サービス提供者に送る手段があるが、IDカードが盗難されたとき紛失した場合、IDキー等でパスワードを入力する行為が、組み合わせにより悪用されるリスクを低減しなければ、盗用する危険が著しく拡大することになる。

【0008】本発明は、上述の点に鑑みてなされたものであり、ネットワークを利用した情報提供サービスにおけるサービス利用者の安全性を向上させること、を目的としてなされたものである。

【0009】

【課題を解決するための手段】請求項1の発明は、MFP、プリンタ等の出力装置とサービス提供者がサービス提供側装置とがネットワークを介して接続され、前記出力装置は、読み取り機能を有し、サービス利用者がサービス提供者の提供したサービスを利用する際に、サービス利用者自身の免許証、保険証、パスポート等の公的な身分証明書を読み取り、読み取った身分証明書の記載内容をネットワークを介して前記サービス提供側装置に送信し、送信された身分証明書の記載内容に基づいてサービス提供者がサービス利用者特定することを特徴としたものである。

【0010】請求項2の発明は、請求項1において、前記出力装置または前記サービス提供側装置は、複数の情報を自動認識する機能を有し、前記身分証明書に記載されている複数のID情報を自動認識し、自動認識された複数のID情報と前記サービス提供側装置に登録されているサービス利用者のID情報とを該サービス提供側装置により突き合わせ、サービス提供者がサービス利用者特定する確度を向上させることを特徴としたものである。

【0011】請求項3の発明は、請求項1において、前記身分証明書の記載内容に基づいてサービス提供者によりサービス利用者が特定されると、当該サービス利用者のサービス受給を承認するためのパスワードが前記サービス提供側装置により生成され、前記出力装置は、紙出力機能を用いて、該生成されたパスワードを前記サービス提供側装置からネットワークを介して受信し、受信したパスワードを紙に出力し、サービス利用者が当該サービスを利用する際に、前記出力した紙に記載されたパスワードを読み取り、読み取ったパスワードをネットワークを介して前記サービス提供側装置に送信し、送信されたパスワードに基づいてサービス提供者がサービス利用者特定することを特徴としたものである。

【0012】請求項4の発明は、請求項3において、前記サービス提供側装置は、前記パスワードを、前記出力装置の読み取り機能により読み取り可能な状態で書き出すことを特徴としたものである。

【0013】請求項5の発明は、MFP、プリンタ等の出力装置とサービス提供者がサービス提供側装置とがネットワークを介して接続され、前記出力装置は、サービス提供者がサービス利用者特定するサービス利用者特定方法であって、前記出力装置は、携帯端末装置に関する固有情報を受信可能なFAX受信機能を有し、サービス利用者が携帯端末装置を用いて当該サービスを利用する際に、サービス利用者の携帯端末装置に関する固有情報を公衆回線を介して受信し、受信した携帯端末装置に関する固有情報をネットワークを介して前記サービス提供側装置に送信し、送信された携帯端末装置に関する固有情報に基づいてサービス提供者がサービス利用者特定することを特徴としたものである。

【0014】

【発明の実施の形態】図1は、本発明が適用されるサービス利用者特定フローの一例を説明する図で、図中、10は、サービス利用側装置である読み取り機能を有するMFP、プリンタ等の出力装置、20は、サービス提供側装置であるサーバ、30は、個人情報記載された免許証、保険証、パスポート等の身分証明書、40は、サービス使用受給通知、50は、ネットワークである。まず、出力装置10で身分証明書30をスキャンし(S1)、前処理として、一次加工(データ補正：MTF等)を行った後、出力装置10の入力データ処理/解析部にて、例えば、像差分、パターン認識、色相差認識、文字認識、番号認識といった二次加工を行うことも出来るが、一次加工したデータをネットワーク50を介してサーバ20に送信し(S2)、後処理として、上記二次加工をサーバ20で行うことも出来る。また、二次加工は、データを認識後、個人情報に必要情報のみを選択し、情報の属性に添付するまでを行うが、出力装置10とサーバ20で分担して行うこともできる。

【0015】このことは、例えば、ISといった規格により認証フォーマットが成立し、そのフォーマットと装置が対応することで汎用的に認証可能となる場合、または、認証フォーマットは未成立だが、装置やサービスを提供する企業間での個別対応により認証を行う場合のいずれにも対応可能とするためである。

【0016】また、こういったフォーマットは暫時変化していくことが想定されるが、サービス利用側機器とサービス提供側機器のいずれかもしくは両方の、ソフトウェアやシステム(ハードウェアを含む)を変更することにより、柔軟に対応可能とすることができ。

【0017】また、ネットワークを介したデータのやり取りを行う際、ネットワークの能力によって処理速度が大きく左右される。当然、サービス利用者、サービス提供者の双方にとって、可能な限り短時間での処理が必然的なニーズとなる。その際、上述のような自由度の高いシステム構成を活用することにより処理時間を短縮化することが可能である

【0018】本例では、出力装置10から送信されたデータの二次加工をサーバ20で行った後に、サーバ20が保持しているサービス利用者の個人情報と突き当て/照合を行って、データが合致した場合に、出力装置10にサービス使用受給通知40を送信する(S3)。

出力装置10は、受信したサービス使用受給通知40を紙に出力し(S4)、サービス利用者がサービス使用受給通知40に同意の意思表示して、例えば、サイン、捺印をした後に、サービス使用受給通知40を出力装置10でスキャンして(S5)、受信受給通知とし、サーバ20へネットワーク50を介して送信し(S6)、サービス提供者は、サービス利用者に対してサービスを開始する。

【0019】(実施例) 図2は、本発明が適用されるシステム構成例を示すブロック図で、出力装置10は、ユーザI/F部11、紙出力部12、紙入力部13、通信I/F部14、機器固有情報記憶部15、サービス関連情報記憶部16、入力データ処理/解析部17を有し、サーバ20は、データ参照部21、入力データ処理/解析部22を有する。

【0020】図3は、本発明が適用されるサービス利用者特定フローの一例を説明するフローチャートである。まず、サービス利用者がサービスを利用するときに、公的に自己を証明可能な免許証、保険証、パスポート等の身分証明書の裏紙や該当ページを開き、公共の場所に設置されている出力装置10のスクリーン上に載せ、例えば、スタートキーを押下げるといった開始の指示をするだけで、入手を介さず行われる。

【0021】スクリーン機能を持つ出力装置10は、載せられた書類のサイズや内容を、センサ手段で認識し、どのような証明書を種類を特定することができる。通常、種類特定後、スキャンを行って、種類特定を目的として行うセンサと同時にスキャンしたり、スキャンを先行し、後に種類特定を行うことも可能である。

【0022】一次加工条件を含むスキャン条件は、あらかじめ最適化されているが、載せられた書類の特性に合わせて自動的にもしくは手動にて最適化することも可能である。

【0023】次に、出力装置10の入力データ処理/解析部17にて一次加工後(ステップS12)、符号化を行って(ステップS13)、機器固有情報記憶部15から機器固有情報を取得し、サービス関連情報記憶部16からデータの送信先を取得して、これらを確認する(ステップS14)。出力装置10は、処理解析済みまたは未処理のデータと、ステップS14で認識した機器固有情報とをネットワーク50を介してサーバ20に送信する(ステップS15)。データを受信したサーバ20は、入力データ処理/解析部22にて二次加工を施して(ステップS16)、データの処理/解析を行う。

【0024】ここで、身分証明書30の特徴は、書式が固定化されているので、どのような証明書が種類を特定

すれば、どの部位に何が記載されているかを判断できる点にある。各証明書に必ず存在する特徴的なアイコンを検出し、そこから位置情報で、利用者の特定の必要な情報を仕置の紋認識し、変換することできる。

【0025】また、前述したように、二次加工は、出力装置10、サーバ20の双方で行うことができる。出力装置10から通信ネットワーク50を介してサーバ20にデータ転送後、サーバ20内のデータ参照部21にて、予め登録されているサービス利用者の個人情報と照し、確認して(ステップS17)、出力装置10から転送された個人情報と、サーバ20内に登録されているサービス利用者の個人情報とが合致するか突き合わせを行って(ステップS18)、合致した場合(YESの場合)は、サーバ20からサービス使用受給通知40が、ネットワーク50を介して出力装置10に対して送信される(ステップS19)。

【0026】一方、出力装置10から転送された個人情報と、サーバ20内に登録されているサービス利用者の個人情報とが合致しなかった場合(YESの場合)は、サーバ20から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される(ステップS20)。尚、この一連の処理は、サービス利用者が有する身分証明書30の裏紙や該当ページを開き、公共の場所に設置されている出力装置10のスクリーン上に載せ、例えば、スタートキーを押下げるといった開始の指示をするだけで、入手を介さず行われる。

【0027】また、他の実施例として、前述したステップS18でサーバ20内のデータ参照部21にて、二次加工後のサービス利用者の個人情報と予め登録されているサービス利用者の個人情報と突き合わせを行う際、取られた少数の情報ではなく、複数の情報と突き合わせを行って、特定の確度を上げるために、図3に示すサブフローのように、予め登録されているサービス利用者の複数のデータを抽出し(ステップS21)、サーバ20内のデータ参照部21にて、順次もしくは同時に突き合わせを行う(ステップS22)。

【0028】ここで、二次加工等の事前の処理において、一つの身分証明書30の裏紙や該当ページから、複数の特定の必要な情報を認識可能であることが効果となる。また、場合によっては、複数の身分証明書30を逆絡めると同時にスキャンし、それらをまたがった突き合わせを行うことにより、更に特定の確度を向上させることが可能である。

【0029】図4は、本発明が適用されるシステム構成例を示すブロック図である。図5は、本発明が適用されるサービス利用側のサービス依頼フローの一例を説明するフローチャートである。サービス利用者とサービス提供者間において、後に発生する可能性が有る請求取回時のトラブルを防止するために、サービス利用者がサービス提供に同意した後に、どのような証明書を種類を特定

10

ードをサービス利用者のサービス利用受諾証明としても使用することができる。

【0041】請求項4の発明によると、サービス利用者は、第三者から取られ、判断不可能な状態に符号化されたパスワードにより、盗用を防止することができる。

【0042】請求項5の発明によると、サービス利用者は、パスワードを公共の場所において10キー等で入力する必要が無く、第三者から盗まれ、盗用される危険を回避できる。

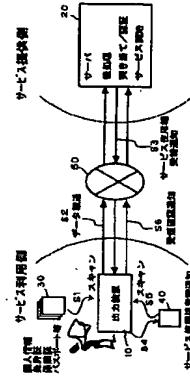
【図面の簡単な説明】

【図1】 本発明が適用されるサービス利用者特定フローの一例を説明する図である。

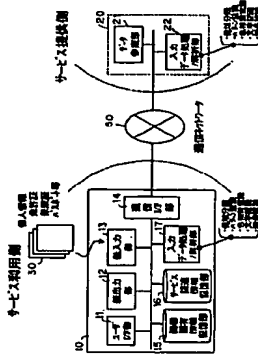
【図2】 本発明が適用されるシステム構成例を示すブロック図である。

【図3】 本発明が適用されるサービス利用者特定フローの一例を説明するフローチャートである。

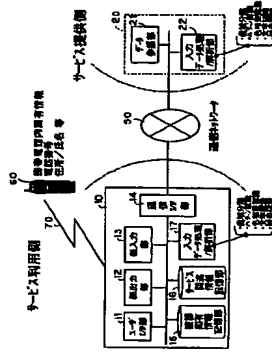
【図1】



【図2】



【図3】



9

知40の発行を行うといった手順も考えられ利用手順を最軽化することも可能である。

【0035】図6は、本発明が適用されるシステム構成例を示すブロック図で、図中、60は、携帯電話、70は、公衆回線である。サービス利用者が所有する携帯電話60の固有情報は、予めサーバ20に登録されており、図6に示すように、サービス利用者は、携帯電話60を用いて公衆回線70を介して出力装置10のFAX番号に電話をかける。サーバ20は、サービス利用者の携帯電話60から提供された機器固有情報を認識し、その情報をサーバ20へ転送する。

【0036】図7は、本発明が適用されるサービス利用者側のサービス依頼フローの一例を説明するフローチャートである。まず、サービス利用者は、サーバ20に登録されているサービス利用者が所有する携帯電話60を利用して公衆回線70を介して出力装置10のFAX番号に電話をかけ（ステップS51）、出力装置10は、携帯電話60の固有情報を認識し（ステップS53）、認識した固有情報を出力装置10の固有情報とをネットワーク50を介してサーバ20に送信する（ステップS54）。サーバ20は、サーバ20内のデータ参照部21にて、予め登録したサービス利用者の携帯電話60の固有情報を参照し、確認して（ステップS55）、出力装置10から転送された携帯電話60の固有情報とサーバ20内に登録されているサービス利用者の個人情報を台合せを行う（ステップS56）、台合した場合（YESの場合）は、サーバ20からサービス使用権受諾通知40が、ネットワーク50を介して出力装置10に対して送信される（ステップS58）。

【0037】一方、ステップS56で台合しなかった場合（NOの場合）は、サーバ20から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される（ステップS57）。

【0038】

【発明の効果】請求項1の発明によると、サービス利用者は、パスワードを公共の場所において10キー等で入力する必要が無く、第三者から取られ、盗用される危険を回避できる。

【0039】請求項2の発明によると、サービス提供者は、複数の情報による利用者特定が可能となり、サービス利用者の免許証、保険証等の身分証明書の偽造による盗用を防止できる。

【0040】請求項3の発明によると、サービス利用者は、パスワードを公共の場所において10キー等で入力する必要が無く、第三者から取られ、盗用される危険を回避でき、サービス提供者から提供されるパスワードは、サービス利用時に改訂可能なため、盗用へのリスクが軽減でき、サービス提供者にとっても、そのパスワード

7

台がある。それに加え、利用者特定の更なる向上が必要なる場合には以下に示す。

【0030】まず、利用者特定の段階として、出力装置10が有する読込機能を用いてサーバ20から伝送されたサービス使用権受諾通知40を出力する（ステップS31）。サービス利用者は、出力されたサービス使用権受諾通知40に、同意の意思表示としてサイン、捺印等を実施する（ステップS32）。ここで、当然理由のみの場合もある。次に、サービス使用権受諾通知40を出力装置10のスクリーン上に載せ開始の指示をする（ステップS33）。ここで、サービス提供者は、サービス使用権受諾通知40にそのサービス利用時の有効なパスワードとして、例えば、数字やバーコードを付加しておくことにより更に特定の精度向上を行うことができる。次に、出力装置10の入力データ処理/解析部17にて一次加工後（ステップS34）、処理解析済データを未処理のデータと、出力装置10の固有情報とをネットワーク50を介してサーバ20に送信する（ステップS35）。データを受信したサーバ20は、入力データ処理/解析部22にて二次加工を施して（ステップS36）、データの処理/解析を行う。

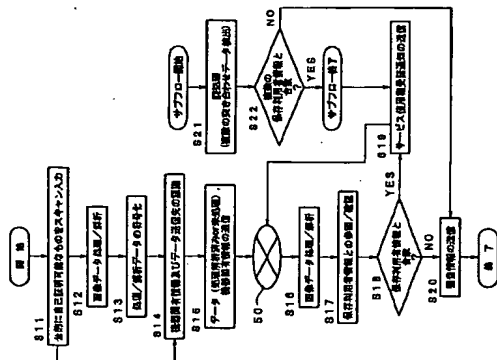
【0031】サーバ20内のデータ参照部21にて、予め登録されているサービス利用者へ提供したパスワード、番号情報を参照し、確認して（ステップS37）、出力装置10から転送されたサービス使用権受諾通知40に付加されたパスワードと、サーバ20内に登録されているサービス利用者のパスワードとを台合せを行う（ステップS38）、台合した場合（YESの場合）は、サービス提供者が提供したサービスがサーバ20よりネットワーク50を介して出力装置10に対して送信される（ステップS40）。

【0032】一方、サービス使用権受諾通知40に付加されたパスワードとサーバ20内に登録されているサービス利用者のパスワードとが台合しなかった場合（NOの場合）は、サーバ20から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される（ステップS39）。

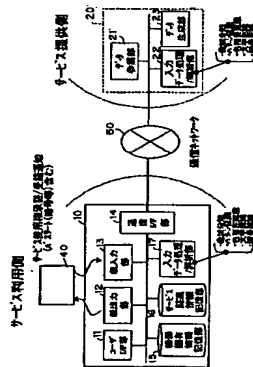
【0033】また、サービス提供者は、サービス利用者がサービス使用権受諾通知40に施した同意の意思表示としてのサインや捺印を利用者特定の情報として活用することもできる。

【0034】上記パスワードとして数字やバーコード以外に、サービス使用権受諾通知40に人が容易に認識できない、もしくは、見ることができない符号で記録し、サービス使用権受諾通知40にサービスメニューを付加し、そのサービスメニューからサービス選択を行なった後、サービス使用権受諾通知40をスクリーン、サーバ20にサービス使用権受諾通知40の発行依頼を行ったり、出力装置10が直接サービス使用権受諾通知40

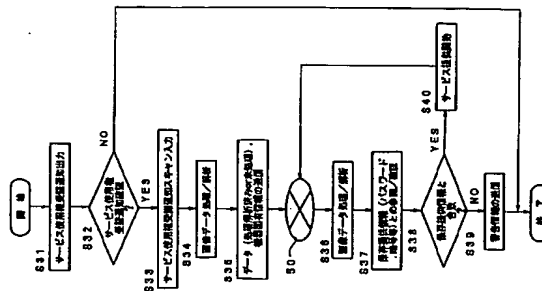
【☒3】



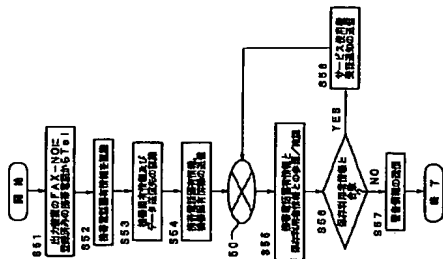
【例4】



【☒5】



【7】



フロントページの続き

Fターム(参考) SB017 AA03 BA05 BA09 CA15 CA16

東京都大田区中馬込1丁目3番6号 株式
会社リコ一内